REMARKS

I. Formalities

Applicant thanks the Examiner for acknowledging the claim for priority under 35 U.S.C. § 119, and receipt of the certified copy of the priority document submitted on October 5, 2000.

Applicant thanks the Examiner for considering the references cited with the Information Disclosure Statement filed on March 9, 2004.

II. Status of the Application

By the present amendment, claims 1-11 have been amended for reasons of grammar and to better conform to U.S. practice. The amendments to claims 1-11 are not made for patentability reasons and do not narrow the scope of the claims. Moreover, claims 12-31 are hereby added to more fully cover various implementations of the invention. Claims 1-31 are all the claims pending in the Application, with claims 1, 6, and 12-29 being in independent form. Claims 1-11 have been rejected.

III. Claim Rejections under 35 U.S.C. §103

The Examiner has rejected claims 1-11 under 35 U.S.C. § 103(a) as being unpatentable over Applicant's admitted prior art, and further in view of U.S. Patent No. 6,453,159 to Lewis (hereinafter "Lewis"). Applicant respectfully traverses this rejection for *at least* the reasons stated below.

In order for the Examiner to maintain a rejection under 35 U.S.C. §103, Applicant's admitted prior art, Lewis, or some combination thereof, must teach or suggest all of the

limitations of claims 1-11. Applicant respectfully submits that neither Applicant's admitted prior art, Lewis, nor any combination thereof, teaches or suggests all of the limitations of claims 1-11.

A. Independent Claim 1

The Examiner takes the position that Applicant's admitted prior art teaches many of the features recited in claim 1, but fails to teach or suggest an authentication server, and the required relationship between the access point and the authentication server. *See* Office Action, page 3, lines 4-5. Applicant agrees with the Examiner that Applicant's admitted prior art fails to teach or suggest these features.

Nevertheless, the Examiner applies Lewis, taking the position that Lewis discloses an authentication server (allegedly key distribution server 76), which interoperates with access points 54 to add a second encryption layer for additional security. Further, the Examiner alleges that one of ordinary skill would have been motivated to modify Applicant's admitted prior art with Lewis in order to maintain a conventional authentication method and network integrity between the terminal station and the access point, while adding additional security to overcome the potential unauthorized or compromising use of the network taught by Lewis. Applicant respectfully disagrees with the grounds of rejection.

Independent claim 1 requires (among other things):

> transmitting an authentication request from a STA (terminal station) to an AP (access point), with which said STA desires to make association; requesting authentication of said authentication request from said AP to an authentication server...

The grounds of rejection allege that the step 224 of Figure 7, as disclosed in Lewis, corresponds to "requesting authentication of said authentication request from said AP to an

authentication server," as recited in Applicant's claim 1. Applicant respectfully disagrees with the grounds of rejection.

Lewis fails to teach or suggest that an authentication request is transmitted from a mobile terminal 66, to an access point 54, and that, in turn, authentication of this authentication request (i.e., an authentication request from the mobile terminal 66 to the access point 54) is requested from the access point 54, to the key distribution server 76 (which the Examiner alleges to correspond to an authentication server as recited in claim 1). To the contrary, Lewis merely teaches that at step 224, if a message received by the access point 54, from a mobile terminal 66, is encrypted using the current ENCRYPT key, then the access point 54 passes this message on to the system backbone 52, and to its intended destination on the system backbone 52. *See* column 13, lines 12-15.

That is, as taught in step 224 of Lewis, after the access point 54 receives a message from a mobile terminal 66 (which the grounds of rejection allege to correspond to an authentication request, as recited in claim 1), Lewis does not teach or suggest requesting authentication of this "authentication request" (i.e., authentication of this message sent by the mobile terminal 66 to the access point 54) from the access point 54 to the key distribution server 76. In fact, step 224 of Lewis teaches quite the opposite—determining whether a message is encrypted using the current ENCRYPT key, and if it is, directly forwarding this message to its intended destination without any processing whatsoever conducted by the key distribution server 76.

Furthermore, as taught in Lewis, the only instance when an access point 54 transmits any sort of message to the key distribution server 76, does not even remotely resemble requesting authentication of an authentication request from an access point to an authentication server, as

recited in claim 1. In particular, Lewis teaches that if an access point 54 determines that a message received from a mobile terminal 66 includes the network address of the key distribution server 76 (e.g., a request for the current ENCRYPT key), the access point 54 will forward the message as originally received onto the system backbone 52, and then to the key distribution server 76. *See* column 13, lines 26-41.

However, as taught in Lewis, this request sent by a mobile terminal 66, for the current ENCRYPT key is not an authentication request. To the contrary, such a request, sent by a mobile terminal 66, for the current ENCRYPT key is, quite simply, a request by the mobile terminal 66 for a data string of auxiliary information that will enable the mobile terminal 66 to communicate with the access point 54 according to a secure encrypted exchange format. *See* column 2, lines 44-51. Indeed, Lewis teaches that a mobile terminal 66 may be authenticated by an access point 54 for communication with the system backbone 52 even if the request by a mobile terminal 66 for the current ENCRYPT key is denied. *See* column 13, lines 23-26. Therefore, Lewis does not teach, and is incapable of suggesting, that the request sent by a mobile terminal 66, for the current ENCRYPT key is an authentication request.

Furthermore, as taught in Lewis, a mobile terminal 66 is not authenticated by the key distribution server 76, rather, a mobile terminal 66 is authenticated by the access point 54 using conventional methods. Specifically, Lewis teaches that each mobile terminal 66 goes through a conventional initialization routine in step 200, whereby the mobile terminal 66 seeks out an access point 54 with which it registers. *See* column 10, lines 54-58. Once this registration between a mobile terminal 66 and an access point 54 is complete, a communication link between the mobile terminal 66 and the access point 54 may be established. *See* column 10, lines 58-63.

Lewis also teaches that, thereafter, the processor 98 within the mobile terminal 66 checks whether the proper MASTER key (necessary for secure access to the network 51 to which the particular access point 54 is connected) has been programmed into the mobile terminal 66 and, if not, processor 98 prompts an operator to input the MASTER key. *See* column 10, line 66 – column 11, line 3; column 11, lines 6-11. Thus, Lewis teaches that if the MASTER key is not input within a predetermined time, the mobile terminal 66 is programmed to shut down. *See* column 11, lines 18-24. Alternatively, if the wrong MASTER key is input, the mobile terminal will not be able to communicate with the network 51. *See* column 11, lines 24-27.

Therefore, Lewis teaches that, by following this conventional initialization routine and process for the verification of the proper MASTER key for communication with the respective network 51, the mobile terminal 66 is authenticated by the access point 54 and may therefore establish communication with the access point 54. Consequently, because the mobile terminal 66 is, in fact, authenticated by the access point 54, the request sent by a mobile terminal 66, for the current ENCRYPT key is clearly not an authentication request.

Additionally, even if this request for the current ENCRYPT key sent from a mobile terminal 66 to an access point 54 did correspond to an "authentication request," which Applicant firmly submits that it does not, Lewis nevertheless fails to teach or suggest, in turn, requesting authentication of this "authentication request" from the access point 54, as required by claim 1. Rather, Lewis teaches just the opposite—that this request for the current ENCRYPT key is sent from a mobile terminal 66, and is addressed to the key distribution server 76. *See* column 13, lines 37-38.

While Lewis may teach that such a request from a mobile terminal 66, to the key distribution server 76, passes through an access point 54 as a passive intermediary, the access point 54 merely forwards the request as originally received onto the system backbone 52, and then to the key distribution server 76. *See* column 13, lines 26-41. Therefore, such a passive forwarding of a request for the current ENCRYPT key, sent from a mobile terminal 66, to the key distribution server 76, by the access point 54, clearly does not meet the requirements of claim 1, which recites requesting authentication of an authentication request from an access point to an authentication server.

For *at least* the reasons set forth above, Lewis fails to teach or suggest transmitting an authentication request from a mobile terminal 66, to an access point 54 and, in turn, requesting authentication of this authentication request (the authentication request from the mobile terminal 66 to the access point 54) from the access point 54, to the key distribution server 76, as required by claim 1.

Independent claim 1 also requires:

> checking said authentication request at said authentication server based on a MAC (media access control) address of said STA;

The Office Action dated April 28, 2004, indicates that Applicant's arguments concerning Applicant's admitted prior art and Lewis are not persuasive. Specifically, the Examiner alleges that Lewis discloses the use of a media access control ("MAC") address as claimed. In particular, the Examiner alleges that the "network addresses or ID's" of the mobile terminals taught in Lewis can be considered MAC addresses, since these identifiers are used to control which packets are transmitted over the network media. *See* Office Action page 10, lines 18-21.

However, Applicant respectfully submits that the Examiner's interpretation of the term "a MAC address," as recited in claim 1, is in error. *See* MPEP § 2111.

Indeed, the Examiner's interpretation of the term "MAC address," to include the "network address or ID" of the mobile terminals taught in Lewis, is not reasonable, as required by MPEP §2111. The "network address or ID" taught in Lewis cannot be a MAC address because it is a local logical identifier that requires manual input by a system administrator.

As explained in the previous Amendment filed on March 17, 2004, the accepted meaning of the term "MAC address" is a globally unique hardware identifier, which is permanently assigned when a device is manufactured and, therefore, cannot be an address which is manually inputted by a system administrator. Indeed, according to the accepted meaning of the term in the art, "a MAC address" typically comprises a 48-bit hexadecimal number (12 characters), and the identifiers taught in Lewis (i.e., "MT1" or "MT2") are clearly not 48-bit hexadecimal numbers.

As exemplary evidence of this accepted definition of "a MAC address," Applicant has submitted along with the present amendment copies of the definition of "a MAC address" from various technical dictionaries. In accordance with MPEP § 2173.05(a), it is appropriate to compare the meaning of terms given in technical dictionaries in order to ascertain the accepted meaning of a term in the art.

In light of these exemplary definitions, it is clear that one skilled in the art would interpret a "MAC address" to mean a globally unique hardware identifier, which is permanently assigned when a device is manufactured. Therefore, Applicant submits that MPEP §2111 requires that any interpretation of the term "a MAC address" adopted by the Examiner must be consistent with this interpretation reached by those skilled in the art. Therefore, a MAC address

cannot be interpreted to mean any address that provides access to the network media, as alleged by the Examiner.

In addition, Applicant submits that the present specification uses the term "a MAC address" consistent with this accepted interpretation. Indeed, Applicant emphatically disagrees with the assertion in the grounds of rejection that the "network address or ID" as taught in Lewis meets the Applicant's own definition of the term "a MAC address." To the contrary, taken in its proper context, the passage of the present specification cited by the Examiner (page 11, lines 28-29) that "the MAC address is defined as a user name or calling station ID on the authentication protocol (RADIUS)," merely connotes that the particular value of the MAC address may be used as the respective values for the "user name" or the "calling station ID" attributes of the authentication information that is used in the RADIUS protocol. Accordingly, Applicant submits that MPEP §2111.01 also requires the Examiner to interpret the term "MAC address," as used in claim 1, in light of the specification's use of the term—which is consistent with the accepted meaning of "MAC address" as discussed above—in giving this term its broadest reasonable interpretation.

In light of the accepted meaning of the term "MAC address," it is clear that Lewis merely teaches that the key distribution server 76 distributes the current ENCRYPT key to mobile terminals 66 based on the contents of system device table 152, which does not include a MAC address. Further, the "network address or ID" taught in Lewis does not inherently include a MAC address because, for the reasons set forth above, the network address or ID taught in Lewis does not necessarily include a MAC address—a determination for which, in relying upon the theory of inherency, the Examiner is required by MPEP §2112 to provide a basis in fact

and/or technical reasoning. To the contrary, the "network address or ID" taught in Lewis is a local logical identifier that requires manual input by a system administrator, whereas a MAC address is a globally unique hardware identifier which is permanently assigned when a device is manufactured and typically consists of a 48-bit hexadecimal number.

Accordingly, Lewis does not teach, and is incapable of suggesting, that the key distribution server 76 checks an authentication request from a mobile station 66 to an access point 54, based on a MAC address of a mobile station 66. Therefore, neither Applicant's admitted prior art, Lewis, nor any combination thereof, teaches or suggests an authentication method comprising checking an authentication request at an authentication server based on a media access control ("MAC") address of a terminal station, as required by Applicant's claim 1.

Thus, Applicant respectfully submits that independent claim 1 is patentable over Applicant's admitted prior art, Lewis, and any combination thereof, for *at least* these reasons. Further, Applicant respectfully submits that the dependent claims 2-5 are allowable, *at least* by virtue of their dependency on claim 1. Consequently, Applicant respectfully requests that the Examiner withdraw this rejection.

B. Independent Claim 6

Independent claim 6 requires (among other things):

> plural APs which connect to an authentication server and said plural STAs, and one of said plural APs receives an authentication request from one of said plural STAs...

In view of the similarity between this requirement and the requirements discussed above with respect to independent claim 1, Applicant respectfully submits that the foregoing arguments as to the patentability of independent claim 1 apply at least by analogy to claim 6.

Specifically, as taught in Lewis, a request sent by a mobile terminal 66, for the current ENCRYPT key is not an authentication request. To the contrary, such a request, sent by a mobile terminal 66, for the current ENCRYPT key, is a request by the mobile terminal 66 for a data string of auxiliary information that will enable the mobile terminal 66 to communicate with the access point 54 according to a secure encrypted exchange format. *See* column 2, lines 44-51.

Furthermore, as taught in Lewis, a mobile terminal 66 is authenticated, not by the key distribution server 76, but by the access point 54 using conventional methods. In particular, Lewis teaches that each mobile terminal 66 is authenticated using a conventional initialization routine and process for the verification of the proper MASTER key for communication with the respective network 51.

As such, it is respectfully submitted that claim 6 is patentably distinguishable over Applicant's admitted prior art, Lewis, and any combination thereof, for *at least* these reasons. Further, Applicant submits that the dependent claims 7-11 are allowable *at least* by virtue of their dependency on claim 6. Thus, the allowance of these claims is respectfully solicited of the Examiner.

IV. New Claims

Claims 12-31 are hereby added and are fully supported by the specificaiton of the instant Application. Claims 12-31 are respectfully submitted to be allowable *at least* by virtue of the recitations set forth therein.

V. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Andrew J. Taska

Andrew J. Taska
Registration No. 54,666

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: July 27, 2004